Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0418U002755

Особливі позначки: відкрита

Дата реєстрації: 02-07-2018

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Ковтун Марія Григорівна
2. Kovtun Mariia

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 05.13.21

Назва наукової спеціальності: Системи захисту інформації

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 27-06-2018

Спеціальність за освітою: Прикладна математика

Місце роботи здобувача: Національний авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: пр. Космонавта Комарова 1, м. Київ, Київ, 03058, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): Д 26.062.17

Повне найменування юридичної особи: Національний авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: пр. Космонавта Комарова 1, м. Київ, Київ, 03058, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Національний авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: пр. Космонавта Комарова 1, м. Київ, Київ, 03058, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 50.37.23

Тема дисертації:

1. Методи удосконалення арифметичних операцій у полях, кільцях та алгебраїчних кривих для криптографічних застосувань

2. Methods of implementation of high speed arithmetic operations in fields, rings and algebraic curves for cryptographic applications

Реферат:

1. Дисертаційна робота присвячена вирішенню актуальної науково-технічної задачі підвищення швидкодії інформаційно-телекомунікаційних систем центрів сертифікації ключів Національної системи електронного цифрового підпису для ДСТУ 4145-2002, ECDSA (IEEE P1363-2000), RSA (IEEE P1363-2000) без фінансових витрат. Підвищення швидкодії операції електронного цифрового підпису полягає в зменшенні обчислювальної складності алгоритмів криптографічних перетворень на основі розробки удосконалених методів та алгоритмів арифметичних операцій над числами, поліномами і точками еліптичних кривих (ЕК), в основному у зменшенні часу виконання трудомісткої операції скалярного множення. В роботі удосконалено метод ділення великих цілих чисел одинарної та подвійної точності на основі алгоритму ділення в стовпчик, що дозволив підвищити швидкодію генерації загальних параметрів криптосистеми RSA. Удосконалено метод здобуття n - го кореня, на прикладі кубічного кореня, який дозволив підвищити швидкодію пошуку

біраціонально еквівалентних кривих Едвардса до кривих Вейерштрасса з ДСТУ 4145-2002 та рекомендованих NIST FIPS 186-4 у двійковому полі. Удосконалено метод інвертування в двійковому полі, вперше розроблено метод побудови алгоритму приведення за фіксованим модулем (три- ,п'ятичленна), що дозволив будувати алгоритми для різних цільових платформ, та удосконалено метод скалярного множення в групі точок еліптичної кривої, за рахунок використання біраціонально еквівалентних кривих Едвардса при операції скалярного множення, що дозволило підвищити швидкодію при формуванні та перевірці ЕЦП згідно ДСТУ 4145-2002 та ECDSA. На основі запропонованих удосконалених методів було розроблено бібліотеку криптографічних примітивів «Cipher+»

2. Thesis is devoted to solving the actual scientific and technical problem of speed-up information and telecommunication systems of the certification authority in National Electronic Digital Signature System for DSTU 4145-2002, ECDSA, RSA without significant financial costs. Speed-up of digital signature operations are in reducing the time of a labor-intensive scalar multiplication operation. The method of dividing large integers of single and double precision based on the school division algorithm is improved. This allows to speed-up of common parameters generation for the RSA cryptosystem. Extracting of n -root method as an example of a cubic root is improved. This allows to speed-up of searching birationally equivalent Edwards curves to Weierstrass curves from DSTU 4145-2002 and recommended by NIST FIPS 186-3 in a binary field. Multiplicative inversion method in a binary field is improved. First proposed method of algorithm building for modular reducing by irreducible polynomial (trinomial, pentanomial) was developed. This allows the constructing of algorithms for various target platforms. Scalar multiplication method in the points group is improved by using birationally equivalent Edwards curves, which allowed to speed-up duration of creation and verification of digital signature in accordance with DSTU 4145-2002 and ECDSA. All proposed methods in dissertation thesis are implemented in library of cryptographic primitives “Cipher+”.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки:

Стратегічний пріоритетний напрям інноваційної діяльності:

Підсумки дослідження:

Публікації:

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації:

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Гнатюк Сергій Олександрович

2. Gnatyuk Sergiy

Кваліфікація: д. т. н., 05.13.21

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Кузнецов Олександр Олександрович
2. Kuznetsov Oleksandr

Кваліфікація: д. т. н., 05.13.21

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Смірнов Олексій Анатолійович
2. Smirnov Oleksiy

Кваліфікація: д. т. н., 21.05.01

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Рецензенти

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Корченко Олександр Григорович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Корченко Олександр Григорович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Т.А.